



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/033,700	12/27/2001	Andre Srinivasan	020581-000600US	8597

31824 7590 10/11/2005

MCDERMOTT WILL & EMERY LLP
18191 VON KARMAN AVE.
SUITE 400
IRVINE, CA 92612-7107

EXAMINER

WORJLOH, JALATEE

ART UNIT	PAPER NUMBER
----------	--------------

3621

DATE MAILED: 10/11/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

ne

Office Action Summary

Application No.

10/033,700

Applicant(s)

SRINIVASAN, ANDRE

Examiner

Jalatee Worjloh

Art Unit

3621

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 14 July 2005.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-3,5-9 and 11-14 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-3,5-9, and 11-14 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Response to Amendment

1. This Office Action is responsive to the amendment filed July 14, 2005, in which claims 1, 7 and 11 were amended and claims 4, 10, 15-19 canceled.

Response to Arguments

2. Applicant's arguments filed July 14, 2005 have been fully considered but they are not persuasive.
3. Applicant amended claim 1 by inserting the limitation of claim 4 and amended claim 7 by included the features of claim 10. Applicant argues that neither Balaz, Cook or Benantar shows or suggests retrieving a second certificate reference to a second certificate wherein the second certificate is issued to an issuer of the first certificate and then transmitting the second certificate reference as part of the message. In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).
4. Claims 1-3, 5-9 and 11-14 have been examined.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

6. Claims 1-3,5,6 and 17 are rejected under 35 U.S.C. 103(a) as being unpatentable over US Publication No. 2004/0177281 to Balaz et al. and US Publication No. 2004/0215959 to Cook et al. in view of US Publication No. 2002/0073310 to Benantar.

Balaz et al. disclose digitally signing a message (i.e. "request") using a first private key associated with the sender (i.e. "router"), see paragraph [0084], retrieving a first certificate reference (i.e. "serial number") associated with a first certificate, the first certificate including a first public key corresponding to the first private key and transmitting to the recipient via the network an authenticated message comprising the digitally signed message and the first certificate reference (see paragraphs [0046], [0085] & [0086]). Balaz et al. disclose a public key infrastructure that comprises a certificate authority that issues the first certificate and the associated first certificate reference (see paragraph [0086]). Balaz et al. do not expressly disclose storing the first certificate and the associated first certificate reference in a public key infrastructure, a second certificate reference associated with a second certificate. Cook et al. disclose the first certificate and the associated first certificate reference are stored in a public key infrastructure (see paragraph [0007] and [0018]). Benantar discloses a second certificate reference associated with a second certificate (see claim 1, lines 4-7). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to modify the method disclose by Balaz et al. to store the first certificate and its reference in a public key infrastructure and a second certificate. One of ordinary skill in the art would have been motivated to do this because it provides a secure system.

Referring to claim 2, Balaz et al. disclose transmitting the first certificate via the network to the public key infrastructure prior to transmitting the authenticated message (see paragraph [0036]).

Referring to claim 3, Balaz et al. disclose the first certificate reference is determined from an identity of the sender and a serial number of the first certificate (see paragraph [0085]).

Referring to claim 5, Balaz et al. disclose the network is the Internet (see paragraph [0032]).

Referring to claim 6, Balaz et al. disclose encrypting the message using a second public key, wherein the recipient holds a second private key corresponding to the second public key (see paragraph [0046]).

Referring to claim 17, Balaz et al. disclose at the sender side: Balaz et al. disclose digitally signing a message (i.e. "request") using a first private key associated with the sender (i.e. "router"), see paragraph [0084], retrieving a first certificate reference (i.e. "serial number") associated with a first certificate, the first certificate including a first public key corresponding to the first private key and transmitting to the recipient via the network an authenticated message comprising the digitally signed message and the first certificate reference (see paragraphs [0046], [0085] & [0086]). Balaz et al. disclose a public key infrastructure that comprises a certificate authority that issues the first certificate and the associated first certificate reference (see paragraph [0086]) and at the recipient side: receiving the message, transmitting the first certificate reference to a public key infrastructure via the network, receiving from the public key infrastructure via the network (see paragraph [0086]) and authenticating the digitally signed message using the first public key (see paragraph [0046]). Balaz et al. do not expressly disclose

Art Unit: 3621

storing the first certificate and the associated first certificate reference in a public key infrastructure. Cook et al. disclose the first certificate and the associated first certificate reference are stored in a public key infrastructure (see paragraph [0007] and [0018]). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to modify the method disclose by Balaz et al. to store the first certificate and its reference in a public key infrastructure. One of ordinary skill in the art would have been motivated to do this because it provides a secure system.

7. Claims 7, 9, 11 and 12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Balaz et al. and US Patent No. 6012039 to Hoffman et al. in view of Benantar.

Referring to claim 7, Balaz et al. disclose transmitting the first certificate reference to a public key infrastructure via the network, receiving from the public key infrastructure via the network a first certificate corresponding to the first certificate reference, the first certificate including a first public key (see paragraph [0086]) and if the first certificate is trusted, authenticating the digitally signed message using the first public key (see paragraph [0046]). Balaz et al. do not expressly disclose determining whether the first certificate is trusted and a second certificate reference associated with a second certificate and a second public key. Hoffman et al. disclose determining whether the first certificate is trusted (see abstract, lines 20-25). Benantar discloses a second certificate and second public key (see claims 1, lines 4-7). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to modify the method disclose by Balaz et al. to include the step of determining whether the

Art Unit: 3621

first certificate is trusted, a second certificate reference and a second public key. One of ordinary skill in the art would have been motivated to do this because it provides security.

Referring to claim 9, Balaz et al. disclose a first certificate (see claim 7 above). Balaz et al. do not expressly disclose identifying a first issuer of the first certificate, comparing the first issuer to each of at least one trusted issuer, and if the first issuer is the same as one of the least one trusted issuer determining that the first certificate is trusted. Hoffman et al. disclose identifying a first issuer of the first certificate, comparing the first issuer to each of at least one trusted issuer, and if the first issuer is the same as one of the least one trusted issuer determining that the first certificate is trusted (see abstract, liens 20-25, col. 13, lines 5-15 and col. 10, lines 34-38). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to modify the method disclose by Balaz et al. to include the steps of disclose identifying a first issuer of the first certificate, comparing the first issuer to each of at least one trusted issuer, and if the first issuer is the same as one of the least one trusted issuer determining that the first certificate is trusted. One of ordinary skill in the art would have been motivated to do this because it prevents fraud and prohibits unauthorized individuals from communicating with the entities in the system.

As for claim 11, see claim 7 rejection above, in which the determination process is taught.

Referring to claim 12, Balaz et al. disclose the network is the Internet (see paragraph [0032]).

8. Claim 8 is rejected under 35 U.S.C. 103(a) as being unpatentable over Balaz et al. , Hoffman et al. and Benantar as applied to claim 7 above, and further in view of Cook et al.

Balaz et al. disclose a public key infrastructure that comprises a certificate authority that issues the first certificate and the associated first certificate reference (see paragraph [0086]).

Balaz et al. do not expressly disclose storing in a local keystore the first certificate and the first public key. Cook et al. disclose storing in a local keystore the first certificate and the first public key (see paragraph [0007] and [0018]). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to modify the method disclose by Balaz et al. to store the first certificate and public key in a local keystore. One of ordinary skill in the art would have been motivated to do this because it provides a secure system

9. Claims 13 and 14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Balaz et al. in view of Benantar.

Referring to claim 13, Balaz et al. disclose determining whether the first certificate reference is stored within a local keystore (*notice, the certificate authority accesses its records to identify the certificate corresponding to the given serial number*), if the first certificate reference is stored within the local keystore: retrieving from the local keystore a first public key associated with the first certificate reference (*the certificate is retrieved which includes the public key and reference*), see paragraph [0086] and if the first certificate reference is not stored within the local keystore: transmitting the first certificate reference to a public key infrastructure, receiving from the public key infrastructure a first certificate, the first certificate including a first public key (see paragraph [0086]). Balaz et al. do not expressly disclose determining whether the first certificate is trusted and adding information to the local keystore, the information including at least the first certificate reference and the first public key. Benantar discloses determining whether the first certificate is trusted and adding information to the local keystore, the information including at

Art Unit: 3621

least the first certificate reference and the first public key (see claims 1 & 7). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to modify the method disclose by Balaz et al. to include the step of determining whether the first certificate is trusted and adding information to the local keystore, the information including at least the first certificate reference and the first public key. One of ordinary skill in the art would have been motivated to do this because it provides security.

Referring to claim 14, Balaz et al. disclose authenticating the digitally signed message using the first public key (see paragraph [0046]).

Conclusion

10. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Art Unit: 3621

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jalatee Worjloh whose telephone number is (571) 272-6714. The examiner can normally be reached on Mondays-Thursdays 8:30 - 7:00.

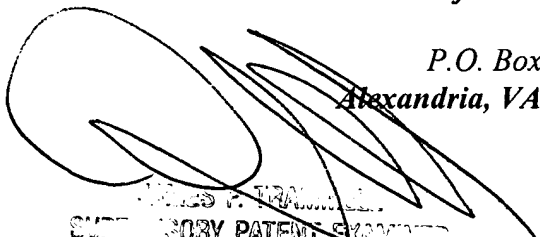
If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, James Trammell can be reached on (571) 272-6712. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300 for Regular/After Final Actions and 571-273-6714 for Non-Official/Draft.


Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Any response to this action should be mailed to:

Commissioner of Patents and Trademarks

*P.O. Box 1450
Alexandria, VA 22313-1450*


JAMES P. TRAMMELL
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 3600


Jalatee Worjloh
Patent Examiner
Art Unit 3621

October 3, 2005